REMARKS

Applicants appreciate the indication that the objection to the Specification and that the rejection under 35 U.S.C. § 101 have been overcome. Applicants, however, submit that the claims are patentable over the cited references for the reasons discussed below. Applicants have amended Claims 1, 22 and 25 to correct grammatical errors in the claims (change "a" to "an").

The Section § 103 Rejections

Claims 1-7, 11-33, 37-48 and 52-57 stand rejected as obvious under 35 U.S.C. § 103 in light of Rivest et al., "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, Vol. 21, Issue 2, February, 1978 (hereinafter "Rivest") and United States Patent No. 6,215,874 to Borza *et al.* (hereinafter "Borza"). Claims 8-10, 34-36 and 49-51 are rejected based on Rivest, Borza and United States Patent No. 6,219,794 to Soutar *et al.* (hereinafter "Soutar").

Claims 1, 22 and 25 Are Patentable Over Rivest and Borza

In rejecting Claims 1, 22 and 25, the Official Action acknowledges that Rivest does not disclose the method used to find random numbers but asserts that Rivest "discloses that to gain additional protection against sophisticated factoring algorithms, p and q should differ in length by a few digits." Official Action, pp. 3-4. The Official Action then concludes that "[b]y finding p and q in different intervals p and q would have different values and therefore different lengths." Official Action, p. 4. The Official Action then states that Borza discloses a method for generating random numbers that uses biometrics. Official Action, p. 4. Finally, the Official Action asserts that Rivest and Borza would be combined because it would reduce the chances of predicting the random number. Official Action, p. 4.

What the Official Action never does is explain where each of the recitations of the claims is found in a cited reference or would result from the combination of references. In particular, the independent claims do not merely recite using a user dependent random number to generate RSA prime numbers but recite specific techniques for generating RSA prime numbers. As discussed in more detail below, these techniques are not disclosed or suggested by Rivest and/or Borza.

The Official Action asserts that because Rivest discloses that the numbers p and q should differ in length, that this suggests the use of different intervals for p and q. Applicants submit that, merely reciting that numbers should differ does not suggest different intervals for the numbers. Claim 1, for example, recites "dividing a potential range of RSA encryption values into a first interval and a second interval." While this division may result in the values differing, other techniques could also result in the values differing and there is no suggestion from the cited references to use different intervals.

Furthermore, Claim 1 does not stop merely with dividing the potential range of values into two intervals but further recites generating initial values, "**mapping** the first initial value to an **entity specific segment of the first interval** utilizing the obtained entity specific information (B) to provide a mapped first initial value (X_p)" and "**mapping** the second initial value to an **entity specific segment of the second interval** utilizing the obtained entity specific information to provide a mapped second initial value (X_q)." Nothing in either Rivest or Borza discloses or suggests a mapping initial values to an entity specific segment of a first interval. The cited portion of Borza merely recites using biometric data to generate a random value. There is no indication in Rivest or Borza that entity specific information is used to map initial values to entity specific segments within an interval as is recited in Claims 1, 22 and 25.

Likewise, there is no suggestion in Rivest or Borza that entity specific segments be used to select starting points for a search for an RSA cryptographic value. Thus, the recitations of "selecting a first user dependent RSA cryptographic value (p) from the entity specific segment of the first interval utilizing the mapped first initial value as a starting point for a search for the first user dependent RSA cryptographic value" and "selecting a second user dependent RSA cryptographic value (q) from the entity specific segment of the second interval utilizing the mapped second initial value as a starting point for a search for the second user dependent RSA cryptographic value" are also not disclosed or suggested by Rivest and/or Borza.

In light of the above discussion, Applicants submit that Claims 1, 22 and 25 and the claims that depend from them are neither disclosed nor suggested by the cited references and, therefore, request withdrawal of the present rejections.

Claims 17, 24 and 27 are Patentable Over Rivest and Borza

In rejecting Claims 17, 24 and 27, the entirety of the rejection is as follows:

> Rivest discloses a method of recovering the cryptographic values p and q by factoring n since it can be done easily once d is known (page 12 section C paragraph 2). The comparison is then an elementary mathematic computation. It is well known that an authentication process includes generating keys that are compared to the expected keys. The keys are determined by the randomized values p and q and therefore the authentic owner would have p and q or a function of p and q.

Official Action, p. 6. However, Claim 17 recites as follows:

> 17. (previously presented)A method of authenticating an RSA cryptographic value comprising the steps of:
>
> recovering two candidate prime values utilizing a RSA public modulus (N) and a private signature exponent (d);
>
> establishing a first of two prime values as a first candidate cryptographic value (p') and the second of the two prime values as a second candidate cryptographic value (q');
>
> recovering first and second candidate seed values W_p' and W_q' from the first and second candidate cryptographic values p' and q' and from the third publicly known seed value IV;
>
> generating first and second RSA cryptographic values p" and q" utilizing W_p' and W_q' and IV; and
>
> comparing p' and p" and q' and q" to authenticate the RSA cryptographic values.

Similar recitations are found in Claims 24 and 27. Applicants submit that even if it is known to generate keys and compare the keys to expected keys, the cited portion of Rivest does not disclose or suggest "recovering first and second candidate seed values W_p' and W_q' from the first and second candidate cryptographic values p' and q' and from the third publicly known seed value IV" and "generating first and second RSA cryptographic values p" and q" utilizing W_p' and W_q' and IV" are cited in Claims 17, 24 and 27. Accordingly, Applicants submit that Claims 17, 24 and 27 are also neither disclosed nor suggested by the cited references.

The Dependent Claims Are Separately Patentable

While each of the dependent claims is patentable as depending from a patentable base claim, Applicants also submit that certain of the dependent claims are also separately patentable over the cited references. For example, Claim 4 recites:

4. (original) A method according to Claim 3, wherein p_0 is a publicly known prime number whose length is at least n bits and g is a public generator, and wherein the step of generating auxiliary prime divisors comprises the steps of:

concatenating the first secret seed value (W_p), the second secret seed value (W_q) and the third randomization value (IV) so as to provide an exponent value (X);

determining an initial random value by determining $Y=g^X(\mathrm{mod}p_0)$;

selecting initial prime search values from the initial random value;

setting the most significant bit of the initial prime search values to "1" to provide final prime search values; and

selecting as the prime divisors the smallest prime value greater than or equal to the final prime search values.

Similar recitations are found in Claims 30 and 45. The Official Action does not cite to any reference as disclosing the recitations of Claims 4, 30 and 45 but merely states that these recitations are "a design choice." Applicants submit that such a conclusory assertion cannot provide the basis of an obviousness rejection. Accordingly, Applicants request that the Examiner either support the assertion by citation to a reference or withdraw the rejection of Claims 4, 30 and 45. Similar unsupported assertions are made with respect to Claims 6, 7, 32, 33, 41, 47, 48 and 56 and these claims are, therefore, also separately patentable for at least these additional reasons.

With regard to Claims 5, 31 and 46, these claims recite criteria for when to re-generate prime divisors. The discussion in the Official Action citing Rivest regarding finding p and q with different lengths does not appear to relate to the recitations of the claims. See Official Action, p. 5. Applicants respectfully submit that to assert that the discussion in Rivest regarding the preference for different length values for p and q teaches the detailed recitations of Claims 5, 31 and 46 is to read too much into the cited portions of Rivest. Accordingly, Applicants submit Claims 5, 31 and 46 are separately patentable over the cited references for at least these additional reasons.

Claims 8, 9 and 10 recite as follows:

8. (original) A method according to Claim 1, wherein the entity specific segments comprise the segments $[A+(B(C-A))/2^b, A+((B+1)(C-A))/2^b]$ wherein A and C are the endpoints of the respective intervals and the entity specific information comprises b bits.

9. (original) A method according to Claim 8, wherein the RSA cryptographic values comprise n bits and wherein the first interval comprises RSA

cryptographic values from the set of $[\sqrt{2}(2^{n-1}), 2^{n-1}+2^{n-3/2}]$ and the second interval comprises RSA cryptographic values from the set of $[\ 2^{n-1}+2^{n-3/2}, 2^{n}\ ]$.

10. (previously presented) A method according to Claim 9, wherein the binary size of the RSA cryptographic values are $2n$, a size m is n-b-2 and wherein the step of mapping the first initial value comprises the steps of:

linearly mapping the first initial value to a entity specific segment of the first interval utilizing the obtained entity specific information (B) utilizing the linear mapping function $G_{1,U}(x) = 4(1 - \frac{1}{\sqrt{2}})x + \sqrt{2}\ 2^{n-1} + 4(1 - \frac{1}{\sqrt{2}})(B-1)2^{m-1}$; and

selecting as the mapped first initial value (X_p) the integer value which is not greater than the first initial value (XX_p)mapped utilizing the mapping function $G_{1,U}$; and

wherein the step of mapping the second initial value comprises the step of linearly mapping the second initial value to a entity specific segment of the second interval utilizing the obtained entity specific information (B) utilizing the linear mapping function; and

selecting as the mapped second initial value (X_q) the integer value which is not greater than the second initial value (XX_q)mapped utilizing the mapping function $G_{2,U}$.

Similar recitations are found in Claims 34-36 and 49-51. The Official Action cites to Figure 1 of Soutar as disclosing the recitations of Claims 8, 34 and 49 stating that "Soutar discloses a method for using a biometric by calculating a values using the information to create a biometric template." Official Action, p. 7. However, the Official Action never indicates where any reference discloses the recitations of Claims 8, 34 and 49. In particular, none of the cited portions of Rivest, Borza or Soutar appear to disclose the specific entity specific segments recited in these claims. Likewise, merely stating the finding p and q in different intervals would result in p and q having different lengths does not disclose or suggest the specific intervals recited in Claims 9, 35 and 50. The Official Action also fails to point to any portion of any reference as disclosing, for example, the mapping function of Claims 10, 36 and 51. Again, the Official Action merely repeats that finding p and q in different intervals would result in p and q having different lengths. The Official Action does not even explain how such a statement would disclose or suggest the recitations of Claims 10, 36 and 51. As such, Applicants submit that Claims 8-10, 34-36 and 49-51 are separately patentable over the cited references for at least these additional reasons.

Claim 13 recites:

13. (original) A method according to Claim 1, further comprising the steps of:

determining if a candidate for p is considered outside the range of RSA cryptographic values in the entity specific segment of the first interval;

selecting at least one of a new first secret seed value (W_p), a new second secret seed value (W_q) and a new third randomization value (IV) if a candidate for p is considered outside the range of RSA cryptographic values in the entity specific segment of the first interval;

determining if a candidate for q is considered outside the range of RSA cryptographic values in the entity specific segment of the second interval;

selecting at least one of a new first secret seed value (W_p), a new second secret seed value (W_q) and a new third randomization value (IV) if a candidate for q is considered outside the range of RSA cryptographic values in the entity specific segment of the second interval; and

restarting the cryptographic value generation utilizing the first and second secret seed values and third randomization value if either a candidate for p is considered outside the range of RSA cryptographic values in the entity specific segment of the first interval or if a candidate for q is considered outside the range of RSA cryptographic values in the entity specific segment of the second interval.

Corresponding recitations are found in Claims 37 and 52. In rejecting Claims 13, 37 and 52 the Official Action again merely asserts that finding p and q in different intervals would result in them having different lengths. No explanation is given to explain how any of the cited references disclose the recitations of Claims 13, 17 and 52, for example, that relate to the determination of whether a candidate values is within the entity specific segments and restarting the cryptographic generation if either candidate value falls outside the entity specific segments. As such, Applicants submit that Claims 13, 37 and 52 are separately patentable for at least these additional reasons.

With regard to Claims 14, 38 and 53, these claims recite, for example, "determining if 2^{16}-1 candidates for p have been rejected in selecting the first user dependent RSA cryptographic value." In rejecting Claims 14, 38 and 53 the Official Action again merely asserts that finding p and q in different intervals would result in them having different lengths. No explanation is given to explain how any of the cited references disclose the recitations of these claims. As such, Applicants submit that Claims 14, 38 and 53 are separately patentable for at least these additional reasons.

Claim 15 recites as follows:

15. (original) A method according to Claim 1, wherein the step of generating a first initial value comprises the steps of:

mixing a concatenation of W_q and IV_q utilizing a publicly known mixing function;

concatenating W_p and IV_p; and

EXCLUSIVE-ORing the mixed concatenation of W_q and IV_q and the concatenation W_p and IV_p to provide the first initial value (XX_p); and

wherein the step of generating a second initial value comprises the steps of:

EXCLUSIVE ORing p and IV_p;

mixing the EXCLUSIVE OR of p and IV_p utilizing the publicly known mixing function;

concatenating W_q and IV_q; and

EXCLUSIVE-ORing the mixed EXCLUSIVE OR of p and IV_p and the concatenation of W_q and IV_q to provide the second initial value (XX_q).

Corresponding recitations are found in Claims 39 and 54 and similar recitations are found in Claims 42 and 57. In rejecting Claims 15, 39, 42, 54 and 57 the Official Action again merely asserts that finding p and q in different intervals would result in them having different lengths. No explanation is given to explain how any of the cited references disclose the recitations of these claims. As such, Applicants submit that Claims 15, 39, 42, 54 and 57 are separately patentable for at least these additional reasons.

Claims 18, 40 and 55 recite "determining that the RSA cryptographic values are not authentic if p' and q' are values outside the user defined segments of the first and second intervals." In rejecting these claims the Official Action states that it is well known that an authentication process includes generating keys that are compared to the expected keys. Official Action, p. 6. However, what the Official Action never does is explain how any of the cited references disclose or suggest also determining if the p and q values are outside the user defined segments and, therefore, would not be authentic even if the recovered and generated p and q values match. Thus, the Official Action has failed to establish how the cited references disclose the recitations of Claims 18, 40 and 55. Accordingly, Applicants submit that Claims 18, 40 and 55 are separately patentable for at least these additional reasons.

Claim 20 recites as follows:

20. (original) A method according to Claim 17, wherein the step of recovering first and second candidate seed values W_p' and W_q' from the first and second candidate cryptographic values p' and q' and from the third publicly known seed value IV comprises the steps of:

inverse mapping the second candidate value q' to provide a first initial value S_q;

EXCLUSIVE ORing the first candidate cryptographic value p' and IV_p;

mixing the EXCLUSIVE OR of the first candidate cryptographic value p' and IV_p with the publicly known mixing function;

EXCLUSIVE ORing the mixed EXCLUSIVE OR of the first candidate cryptographic value p' and IV_p with IV_q to provide a first known value (N_q) having a length (j);

determining if a value corresponding to the j least significant bits of S_q is less than the first known value N_q;

EXCLUSIVE ORing the n-j most significant bits of the mixed concatenation of the first candidate cryptographic value p' and IV_p with the n-j most significant bits of S_q if the value corresponding to the j least significant bits of the first subsequent value is not less than the first known value N_q, to provide the second candidate seed value;

EXCLUSIVE ORing the n-j most significant bits of the mixed concatenation of the first candidate cryptographic value p' and IV_p with 1 subtracted from the value corresponding to the n-j most significant bits of S_q if the value corresponding to the j least significant bits of the first subsequent value is less than the first known value N_q, to provide the second candidate seed value;

inverse mapping the first candidate value p' to provide a second initial value S_p;

concatenating the second candidate seed value and IV_q;

mixing the concatenation of the second candidate seed value and IV_q with the publicly known mixing function;

EXCLUSIVE ORing the mixed concatenation of the second candidate seed value and IV_q with IV_p to provide a second known value N_p having a length (j);

determining if a value corresponding to the j least significant bits of S_p is less than the second known value N_p;

EXCLUSIVE ORing the n-j most significant bits of the mixed concatentation of the second candidate seed value and IV_q with the n-j most significant bits of S_p if value corresponding to the j least significant bits of the second subsequent value is not less than the second known value N_p, to provide the first candidate seed value;

EXCLUSIVE ORing the n-j most significant bits of the mixed concatenation of the second candidate seed value and IV_q with 1 subtracted from the value corresponding to the n-j most significant bits of S_p if the value corresponding to the j least significant bits of the second subsequent value is less than the second known value N_p, to provide the first candidate seed value.

In rejecting Claim 20 the Official Action again merely asserts that finding p and q in different intervals would result in them having different lengths. No explanation is given to explain how any of the cited references disclose the recitations of Claim 20. As such, Applicants submit that Claim 20 is separately patentable for at least these additional reasons.

Conclusion

In light of the above discussion, Applicants submit that the present application is in condition for allowance, which action is respectfully requested.

Respectfully submitted,

Timothy J. O'Sullivan
Registration No. 35,632

Customer No. 20792
Myers Bigel Sibley & Sajovec
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401

Certificate of Mailing under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Non-Fee Amendment, Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450 on February 18, 2004.

Traci A. Brown